CLAIMS

1. An information-processing apparatus used for carrying out a process to decrypt encrypted data stored on an information-recording medium, said information-processing apparatus having encryption-processing means for:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 by carrying out an encryption process based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium based on said generated second block key Kb2.

2. The information-processing apparatus according to claim 1, said information-processing apparatus having storage means for storing master-key generation

information, wherein said encryption-processing means:

generates a master key on the basis of said master-key generation information;

generates two recording keys K1 and K2 on the basis of said generated master key and information read out from said information-recording medium;

generates a first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

acquires a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generates a second block key Kb2 by carrying out an encryption process based on said acquired second seed and said generated second recording key K2; and

decodes encrypted data stored on said information-recording medium by carrying out a decryption process based on said generated second block key Kb2.

3. The information-processing apparatus according to claim 2 wherein said encryption-processing means also:

generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-

recording medium, and two title keys recorded on said information-recording medium;

generates a first recording key K1 by carrying out an encryption process based on said first title unique key and first information read out from said information-recording medium; and

generates a second recording key K2 by carrying out an encryption process based on said second title unique key and second information read out from said information-recording medium.

4. The information-processing apparatus according to claim 2 wherein said encryption-processing means also:

generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and one key seed recorded on said information-recording medium;

generates a first recording key K1 by carrying out an encryption process based on said first title unique key and first information read out from said information-recording medium; and

generates a second recording key K2 by carrying out an encryption process based on said second title unique key and second information read out from said

information-recording medium.

5. An information-recording medium drive used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-recording medium drive comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

encryption-processing means for:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1; and

generating output-use encrypted information by carrying out a process to encrypt data including said second seed on the basis of said session key Ks,

wherein said output-use encrypted information obtained as a result of said process to encrypt data including said second seed on the basis of said session key Ks is output through an interface.

6. The information-recording medium drive according to claim 5 wherein said encryption-processing means also:

generates a master key on the basis of master-key generation information held by said information-recording medium drive;

generates two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

generates a first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

acquires a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generates output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

outputs said output-use encrypted information including said second seed and said second recording key K2 through an interface.

7. An information-processing apparatus used for carrying out a process to decrypt encrypted data received from an external apparatus through a data input interface, said information-processing apparatus comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus outputting said encrypted data in order to generate a session key Ks; and

an encryption-processing unit for:

acquiring a seed used as key generation information and a recording key by carrying out a process based on said session key to decrypt encrypted information received through said data input interface;

generating a block key to be used as a decryption key for decryption of encrypted data by carrying out an encryption process based on said seed and said recording key; and

carrying out a process based on said block key to decrypt encrypted data.

8. An information-recording medium drive used for reading out encrypted data from an information-recording

medium and outputting said encrypted data to an external apparatus, said information-recording medium drive having a configuration comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

encryption-processing means for:

generating a block key on the basis of a seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring decrypted data by carrying out a process to decrypt said encrypted data stored on said information-recording medium on the basis of said generated block key; and

generating output-use encrypted information by carrying out a process to encrypt said decrypted data on the basis of said generated session key Ks,

wherein said output-use encrypted information obtained as a result of said process to encrypt said decrypted data on the basis of said session key Ks is output through an interface.

9. An information-recording medium used for storing encrypted data, said information-recording medium comprising a configuration for storing:

a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data;

a second seed serving as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed; and

an encrypted content encrypted on the basis of a second block key Kb1 generated on the basis of said second seed.

10. The information-recording medium according to claim 9 wherein said first seed is stored inside control information set for each of encryption-processing units whereas said second seed is stored as encrypted information in a user-data area outside said control information.

11. The information-recording medium according to claim 9 wherein said first seed is stored in a user-data area as unencrypted data whereas said second seed is stored in said user-data area as encrypted data.

12. The information-recording medium according to claim 9 wherein said encrypted data is a transport stream

packet, said first seed is stored inside control information for a plurality of transport stream packets, and said second seed is stored as encrypted information inside one of said transport stream packets in a user-data area outside said control information.

13. The information-recording medium according to claim 9 wherein said first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas said second seed is stored as encrypted information inside said transport stream packet in said user-data area.

14. An information-processing method used for carrying out a process to decrypt encrypted data stored on an information-recording medium, said information-processing method comprising the steps of:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium by carrying out a decryption process based on said generated second block key Kb2.

15. The information-processing method according to claim 14, said information-processing method further having the steps of:

generating a master key on the basis of master-key generation information read out from storage means;

generating two recording keys K1 and K2 on the basis of said generated master key and information read out from said information-recording medium;

generating a first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 by carrying out an encryption process based on said acquired second seed and said generated second recording key K2; and

decrypting said encrypted data stored on said

information-recording medium by carrying out a decryption process based on said generated second block key Kb2.

16. The information-processing method according to claim 15, said information-processing method further having the steps of:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and two title keys recorded on said information-recording medium;

generating a first recording key K1 by carrying out an encryption process based on said first title unique key and first information read out from said information-recording medium; and

generating a second recording key K2 by carrying out an encryption process based on said second title unique key and second information read out from said information-recording medium.

17. The information-processing method according to claim 15, said information-processing method further having the steps of:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-

recording medium, and one key seed recorded on said information-recording medium;

generating a first recording key K1 by carrying out an encryption process based on said first title unique key and first information read out from said information-recording medium; and

generating a second recording key K2 by carrying out an encryption process based on said second title unique key and second information read out from said information-recording medium.

18. An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising the steps of:

carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating output-use encrypted information by carrying out a process to encrypt data including said second seed on the basis of said session key Ks; and

outputting said output-use encrypted information obtained as a result of said process to encrypt data including said second seed on the basis of said session key Ks through an interface.

19. The information-processing method according to claim 18, said information-processing method further having the steps of:

generating a master key on the basis of master-key generation information held by an information-recording medium drive;

generating two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

generating a first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

acquiring a second seed by carrying out a process

to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

outputting said output-use encrypted information including said second seed and said second recording key K2 through an interface.

20. An information-processing method used for carrying out a process to decrypt encrypted data received from an external apparatus through a data input interface, said information-processing method comprising the steps of:

carrying out an authentication process with said external method outputting said encrypted data in order to generate a session key Ks;

acquiring a seed used as key generation information and a recording key by carrying out a process based on said session key to decrypt encrypted information received through said data input interface;

generating a block key to be used as a decryption key for decryption of encrypted data by carrying out an

encryption process based on said seed and said recording key; and

carrying out a process based on said block key to decrypt encrypted data.

21. An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising the steps of:

carrying out an authentication process with said external method to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks;

generating a block key on the basis of a seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring decrypted data by carrying out a process to decrypt encrypted data stored on said information-recording medium on the basis of said generated block key;

generating output-use encrypted information by carrying out a process to encrypt said decrypted data on the basis of said generated session key Ks; and

outputting said output-use encrypted information obtained as a result of said process to encrypt said decrypted data on the basis of said session key Ks through an interface.

22. A computer program to be executed for carrying out a process to decrypt encrypted data stored on an information-recording medium, said computer program comprising the steps of:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium by carrying out a decryption process based on said generated second block key Kb2.